

REMARKS

Claim Status

Upon entry of this amendment, claims 1, 7 and 11 have been amended, claims 4, 10 and 15-19 have been canceled; claims 1-3, 5-9 and 11-14 remaining pending.

35 USC 112 Rejection

Claim 11 is rejected under 35 USC 112 as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. More specifically, claim 11 is rejected on the basis that it does not provide steps if the second certificate is not trusted. It is believed that the amended claim 11 is now sufficient to traverse the foregoing rejection. Therefore, Applicant respectfully submits that the foregoing rejection should now be withdrawn.

35 USC 102 Rejection

Claims 18 and 19 are rejected under 35 USC 102(e) as being anticipated by Balaz et al. (US Publication No. 2004/0177281). In the interest of expediting allowance of the present application and without conceding the issue of patentability, Applicant has canceled claims 18 and 19. Therefore, the foregoing rejection is now moot.

35 USC 103 Rejection

Claims 1-3, 5, 6 and 17 are rejected under 35 USC 103(a) as being unpatentable over Balaz et al. in view of Cook et al. (US Publication No. 2004/0215959).

With respect to claim 1, this claim has been amended to include limitations from claim 4. As will be further discussed below in connection with claim 4, Applicant respectfully submits that claim 1 as amended is now patentable over the cited art.

With respect to claims 2 and 3, these claims depend from claim 1 and therefore at least derive their patentability therefrom. Notwithstanding the foregoing, these claims on their own are also patentable over the cited art. Regarding claim 2, it is alleged that Balaz et al. discloses transmitting the first certificate via the network to the public key infrastructure prior to transmitting the authenticated message. Further review of the cited excerpt, paragraph [0036], does not support the foregoing position. Paragraph [0036] merely shows that each router is assigned a unique

certificate. As stated in the Examiner's arguments in connection with claim 1, a router as identified by the Examiner is the sender. As recited in claims 1 and 2, the sender is not the same as the public key infrastructure. Therefore, Balaz et al. does not disclose or suggest the limitations as recited in claim 2. Hence, claim 2 on its own is also patentable over the prior art. Regarding claim 3, it is alleged that Balaz et al. discloses that the first certificate reference is determined from an identity of the sender and a serial number of the first certificate. Further review of the cited excerpt, paragraph [0085], does not support the foregoing position. Paragraph [0085] does not disclose or suggest using the identity of the sender to determine the first certificate reference. Therefore, Balaz et al. does not disclose or suggest the limitations as recited in claim 3. Hence, claim 3 on its own is also patentable over the cited art.

With respect to claims 5 and 6, these claims depend from claim 1 and therefore at least derive their patentability therefrom. Hence, claims 5 and 6 are also patentable over the cited art.

With respect to claim 17, in the interests of expediting allowance of the present application and without conceding the issue of patentability, this claim has been canceled. Therefore, the foregoing rejection with respect to claim 17 is now moot.

Claim 4 is rejected under 35 USC 103(a) as being unpatentable over Balaz et al. and Cook et al. and further in view of Benantar (US Publication No. 2002/0073310). It should be noted that claim 4 has been incorporated into claim 1. Therefore, the following discussion is applicable to claim 1. It is alleged that Benantar discloses a second certificate reference associated with a second certificate. However, a second certificate reference is not all that is recited in claim 4. One or more of the features recited in claim 4 are not disclosed or suggested by Balaz et al., Cook et al. and Benantar. For example, none of these references shows or suggests retrieving a second certificate reference to a second certificate wherein the second certificate is issued to an issuer of the first certificate and then transmitting the second certificate reference as part of the message. Therefore, the first and second certificates are related and the message has both first and second certificate references. Hence, claim 4, vis-à-vis, claim 1 as amended is patentable over the cited art.

Claims 7, 9 and 12 are rejected under 35 USC 103(a) as being unpatentable over Balaz et al. in view of Hoffman et al. (U.S. Pat. No. 6,012,039). With respect to claim 7, this claim has been amended to include limitations from claim 10. As will be further discussed below in connection with claim 10, Applicant respectfully submits that claim 7 as amended is now patentable over the

cited art. With respect to claims 9 and 12, these claims depend from claim 7 and therefore at least derive their patentability therefrom. Hence, claims 9 and 12 are also patentable over the cited art.

Claim 8 is rejected under 35 USC 103(a) as being unpatentable over Balaz et al. and Hoffman et al. and further in view of Cook et al. Claim 8 depends from claim 7 and therefore at least derives its patentability therefrom. Hence, claim 8 is also patentable over the cited art.

Claims 10 and 11 are rejected under 35 USC 103(a) as being unpatentable over Balaz et al. and Hoffman et al. and further in view of Benantar. With respect to claim 10, this claim has been incorporated into claim 7. Therefore, the following discussion is applicable to claim 7. It is alleged that Benantar discloses a second certificate reference associated with a second certificate. However, a second certificate reference is not all that is recited in claim 10. One or more of the features recited in claim 10 are not disclosed or suggested by Balaz et al., Hoffman et al. and Benantar. For example, none of these references shows or suggests transmitting a second certificate reference to a public key infrastructure and then receiving the second certificate where the second certificate includes a second public key that is associated with an issuer of the first certificate. Therefore, the first and second certificates are related and the message has both first and second certificate references. Hence, claim 10, vis-à-vis, claim 7 as amended is patentable over the cited art.

With respect to claim 11, this claim depends from claim 7 and therefore at least derives its patentability therefrom. Hence, claim 11 is also patentable over the cited art. Notwithstanding the foregoing, claim 11 on its own is also patentable over the cited art. It is alleged that Balaz et al. and Hoffman et al. disclose the features as recited in claim 11. Further review of these references shows the contrary. The cited excerpts from Hoffman et al. merely show that a digital certificate can be used to identify an issuer. These excerpts do not show or suggest using a second certificate to authenticate a first certificate. Hence, claim 11 on its own is also patentable over the cited art.

Claims 13 – 16 are rejected under 35 USC 103(a) as being unpatentable over Balaz et al. in view of Benantar. With respect to claim 13, it is alleged that Balaz et al. discloses determining whether the first certificate reference is stored within a local keystore and also a number of steps to be performed if the first certificate reference is not stored within the local keystore. Further review of the cited excerpt, paragraph [0086], shows that the Examiner's position is inconsistent. For example, as discussed in the arguments in connection with claim 8, the Examiner identified the certificate authority as the public key infrastructure. Now the Examiner appears to take the position

that the certificate authority is the local keystore. The certificate authority cannot be both at the same time. Furthermore, even assuming that the certificate authority was the local keystore, paragraph [0086] merely shows the certificate authority returning a certificate. If the certificate authority was the local keystore, then paragraph [0086] does not disclose or suggest a public key infrastructure and that the public key infrastructure is to be contacted if a certificate reference is not stored in the local keystore. The certificate authority cannot be both the local keystore and the public key infrastructure at the same time. Hence, claim 13 is patentable over the cited art.

With respect to claim 14, this claim depends from claim 13 and therefore at least derives its patentability therefrom. Hence, claim 14 is patentable over the cited art.

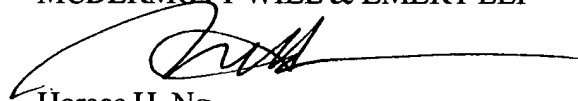
With respect to claims 15-16, in the interests of expediting allowance of the present application and without conceding the issue of patentability, Applicant has canceled claims 15 and 16. Therefore, the foregoing rejection with respect to these claims is now moot.

Conclusion

In view of the foregoing, Applicant believes all claims now pending in this application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested. If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at the telephone number provided below.

Respectfully submitted,

MCDERMOTT WILL & EMERY LLP



Horace H. Ng
Registration No. 39,315

18191 Von Karman Ave., Suite 400
Irvine, CA 92612-7107
Telephone: 949.851.0633
Facsimile: 949.851.9348
HN:al

Date: July 12, 2005

MPK 88240-1.072130.0025